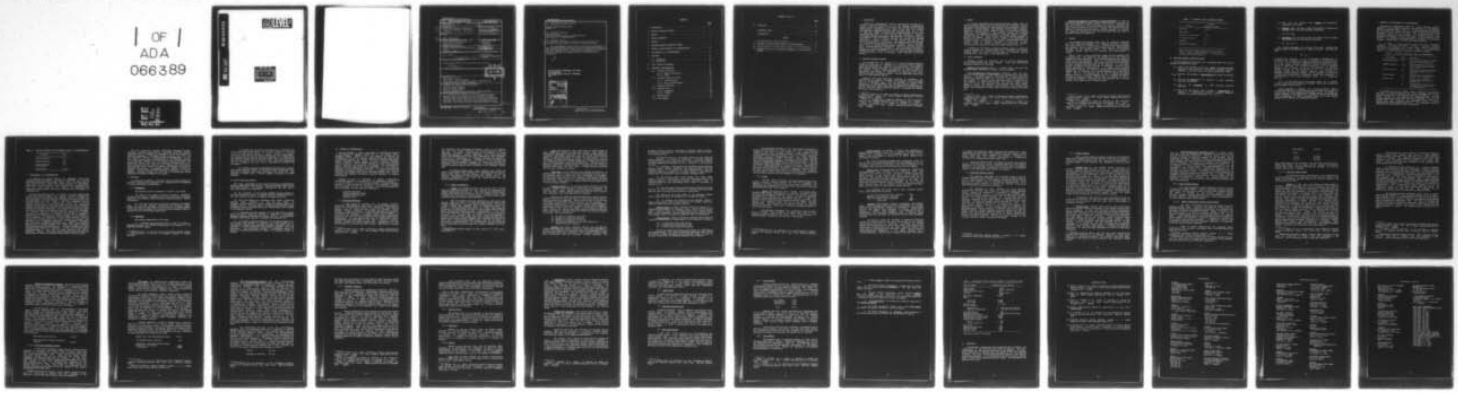
AD-A066 389 HARRY DIAMOND LABS ADELPHI MD F/G 17/2
IMPACT OF SABOTAGE ON MANNED DCS FACILITIES - TASK II: COST-BEN--ETC(U)
NOV 78 M B GINSBERG
UNCLASSIFIED HDL-TM-78-13 SBIE -AD-E100 165 NL

1 OF 1
ADA
066389



END
DATE FILMED
5-79
DDC

(12) LEVEL III

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: HDL-TM-78-13	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle): Impact of Sabotage on Manned DCS Facilities— Task II: Cost-Benefit Analysis.	5. TYPE OF REPORT & PERIOD COVERED: Technical Memorandum
6. PERFORMING ORG. REPORT NUMBER	
7. AUTHOR(s): Murry B. Ginsberg	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Harry Diamond Laboratories, 2800 Powder Mill Road, Adelphi, MD 20783	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: Program Ele: 3.31.26K
11. CONTROLLING OFFICE NAME AND ADDRESS: Defense Communications Engineering Center, Reston VA, 22090	12. REPORT DATE: November 1978
	13. NUMBER OF PAGES: 39
14. MONITORING AGENCY NAME & ADDRESS (If different from Controlling Office): SBIE; AD-E100 165	15. SECURITY CLASS. (of this report): UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

44p.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

DDC RECEIVED MAR 27 1979 B

18. SUPPLEMENTARY NOTES

HDL Project: W247W2
DRCMS Code: 36AA.71.0033126
This research was sponsored by Defense Communications Engineering Center, (cont'd on back)

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Sabotage of communications facilities
Security system concepts
Security system elements
Security system costs
Saboteur-defender interaction model (cont'd on back)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A cost-benefit analysis is made of potential counter-measures (CM's) to increase the survivability of Defense Communications System (DCS) sites to an attack by saboteurs. The objectives of the security system and augmenting CM's are examined, the threat is outlined, and attack deterrents are specified. The estimated times to sabotage potential targets (over)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

163 050 LB

18. Supplementary Notes (Cont'd)

Defense Communications Agency
Reston, VA

19. Key Words (Cont'd)
Site protection
Measure of effectiveness of countermeasures
Cost-benefits of countermeasures

20. Abstract (Cont'd)
are tabulated. An attacker-defender interaction model and measures of effectiveness of potential CM's are defined.

The requirements of the security system and its elements are described considering different levels of system sophistication. The estimated unit costs of these potential elements are tabulated. The user responsibility is to balance an acceptable level of protection against an acceptable level of expenditures for protection.

RE: Classified references, distribution unlimited-
No change per Mr. Murry B. Ginsberg, HDL

CONTENTS

CONTENTS (Cont'd)

TABLES

1. INTRODUCTION

As part of a comprehensive effort to increase the survivability of existing world-wide facilities of the DCS (Defense Communications System) to acts of sabotage, a four-part study was made for the Defense Communications Engineering Center. First, a site survey and analysis was conducted of unmanned DCS facilities (microwave radio relay sites) in CONUS and Europe, to identify site susceptibilities and potential countermeasures (CM's) to curb sabotage and vandalism.[1] Second, a cost-benefit analysis methodology was developed to determine the most cost-effective CM's for curbing vandalism and sabotage at unmanned facilities.[2] Third, a series of site surveys and analyses was conducted of manned DCS facilities in the European and Pacific theaters (1) to identify site susceptibilities and potential CM's to curb sabotage and (2) to develop sabotage attack scenarios, physical security SOP's (Standard Operating Procedures), and Site Security Checklists.[3] Finally, in the study reported here, a cost-benefit analysis is made to determine the most cost-effective CM's for upgrading the survivability of DCS facilities to acts of sabotage. (Cost estimates are in 1977 dollars.)

2. PHYSICAL PROTECTION SYSTEM

It is assumed that the objective of a site's physical protection system is to curb acts of sabotage by an external threat aimed at disrupting communications. Therefore, the system should be designed to deter, detect, impede, intercept, and neutralize an attacker before he can sabotage a site's operating components. CM's can enhance communications survivability by augmenting the capabilities of a site's existing physical protection system. Such an enhancement should take place in a cost-effective manner.

Potential CM's entail three basic functions or parameters: the detection of the attacker, the delay of the attacker, and the response time of the defender. Thus, CM's are designed to achieve three objectives: (1) provide earlier, more reliable intrusion detection (2) increase the time it takes the attacker to complete his sabotage mission and (3) reduce the time it takes the defender to intercept the attacker following a valid detection.

---

[1] *Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)*

[2] *Murry B. Ginsberg et al, Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977). (FOUO)*

[3] *Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)*

3. THREAT

It is quite conceivable that concerted sabotage attacks might be directed against several sites with the purpose of disrupting the DCS. Such attacks would probably be perpetrated by trained sabotage teams of dedicated, well-disciplined, well-equipped, and well-armed personnel. Examples of typical attack scenarios drawn up by potential sabotage teams are given elsewhere.[1,3] The scenarios contain the following information: the manpower and materiel resources needed to conduct sabotage missions, the likely targets, and the time needed to damage or destroy the targets. There is also, however, the possibility of terrorist attacks. Terrorists--who have more limited capabilities and objectives than the sabotage teams--might, for political or other reasons, attempt to damage or destroy DCS facilities. However, terrorists may be deterred by relatively modest measures (sect. 4).

In addition to the threat of external sabotage, there is a threat of internal sabotage, i.e., sabotage from within. Presumably, the internal sabotage threat can best be curbed by means of personnel security investigations. This threat is not addressed here.

4. ATTACK DETERRENTS

Sabotage, at least by terrorists, may be curbed by implementing policies with measures that deter attacks. Three such policies and associated measures are indicated:

Maintain a low profile.--Keep to a minimum number the signs that identify a site, its location, mission, and key personnel.

Give the appearance of good security.--Present at least the illusion, if not the reality, of good security by implementing the following measures: a formidable appearing, well-maintained perimeter fence that is kept well lighted at night; an adjoining, large level area that is kept cleared, i.e., free of foliage and obstructions to visibility; and the presence of armed security guards. The security guards should appear to follow good practices and procedures and should conduct perimeter patrols and periodic sabotage alerts. Also, display signs should warn trespassers of deadly force, electrified fencing, and guard dogs.

---

[1] *Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)*

[3] *Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)*

Promote the community's interest in site survivability.--It may be possible and desirable to allow a site's microwave tower to be shared by such local community services as medical, fire, police, telephone, and radio and TV services. (Only the antennas and connecting waveguides and cables should be allowed on the site.) However, the benefits and risks inherent in sharing the tower must be carefully weighed. For example, the community's dependence on the tower may actually make the tower an attractive target for anarchists.

5. TARGETS

Site components and equipment that might be targeted by saboteurs have been identified elsewhere.[1-3] For unmanned facilities (microwave relay sites) where it is unlikely that a reaction force could intercept the saboteurs quickly enough, the microwave tower and communications equipment are the probable targets. Such targets are considered lucrative, because they would be expensive and time-consuming to replace.

Table I lists a range of potential targets and the estimated times to sabotage them. The saboteurs are assumed to be well armed and equipped with high explosives. The estimated sabotage times reflect an attack that is quasi-unopposed. That is, we assume that the defenders cannot obstruct the saboteurs. The threat-target interactions indicated in table I presume site penetration by the saboteur. In some cases, however, the saboteur may not even need to penetrate the site to cause serious disruption of communications. For example, sites containing troposcatter antennas or satellite antennas that are not enclosed by radomes may be vulnerable to an offsite marksman with a high-powered rifle. That is, the marksman may be able to destroy the antenna feedhorn, which is a crucial component that is not readily replaceable. The physical protection system studied here is designed to curb an attacker who attempts to penetrate the site perimeter, and it has only limited utility against such a standoff attack.

---

[1] *Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)*

[2] *Murry B. Ginsberg et al, Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977). (FOUO)*

[3] *Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)*

TABLE I. ESTIMATED TIMES TO SABOTAGE TARGETS

Target	Estimated sabotage time[a] (min)
Tower legs	5 to 15
Power cables	15
Generators & switching gear	5 to 8
Air-conditioning units	5 to 8
Waveguides	5
Communications equipment	15

[a] *Total time, including fence penetration and on-site transit times, for saboteur (assumed unopposed) to place explosives charges on target and damage or destroy it. The Special Forces, Ft. Bragg, provided time estimates.*

6. ATTACKER-DEFENDER INTERACTION MODEL

The time parameters associated with a sabotage attack and a site's defense are defined as follows

t_t = time for the attacker to reach the target following perimeter penetration (and potential activation of perimeter intrusion sensors); t_t includes transit and barrier penetration times.

$t_{d/d}$ = time for the attacker to damage/destroy the target on reaching it.

t_d = time till the detection of an intrusion is made, following perimeter penetration.

t_a = time till the assessment is made, following intrusion detection.

t_c = time till the reaction force receives a communication to respond to an unauthorized intrusion, following detection assessment (t_c assumed negligible, i.e., $t_c = 0$).

t_r = time till the reaction force responds and potentially intercepts the attacker.

T_s = sabotage time: the time it takes the attacker to complete the sabotage mission following perimeter penetration.

$$T_s = t_t + t_{d/d}$$

T_e = engagement time: the time it takes the reaction force to engage the attacker following perimeter penetration.

$$T_e = t_d + t_a + t_r$$

For a timely engagement, the reaction force must intercept the attacker before he has completed his sabotage mission. This requires that

$$T_e < T_s \quad .$$

To satisfy this condition, it may be necessary to implement CM's to increase T_s (by increasing t_t or $t_{d/d}$) or decrease T_e (by decreasing t_d, t_a, or t_r). It is difficult to determine whether the intercept criterion is met, however, because t_d depends on a random variable, the probability of detection. To avoid this difficulty, use the following approach: let t_d include t_a, and let the probability of detection account entirely for the variability of t_d. To illustrate this approach, assume that the physical security system is based on a perimeter intrusion-detection system, and the assessment of a detection is essentially instantaneous. Furthermore, assume the probability of detection is P_d; if a valid detection occurs, $t_d = 0$ (therefore, $T_e = t_r$).

If $T_e < T_s$, the probability of interception equals P_d. In essence, we have transformed the parameters of interest from t_d and t_a--which we have set equal to zero--to P_d.

Timely engagement is necessary, but it does not suffice. Namely, the reaction force must be sufficiently potent to defeat an attacker, or it must delay him until adequate reinforcements arrive. To successfully thwart saboteurs, it may therefore be necessary to upgrade the reaction force's capability to repel an attacker, where P_r is the present probability of repelling an intercepted attacker.

7. MEASURE OF EFFECTIVENESS OF COUNTERMEASURES

The measure of effectiveness (MOE) of a site's security system is embodied in the parameters defined and discussed in the attacker-defender interaction model (sect. 6). It may be necessary to implement CM's to enhance the security system's effectiveness by changing these parameters. Each CM has an MOE which can be described by one of the following parameters: a time increment in an attacker's action, a time decrement in a defender's action, an increase in the probability of detection, or an increase in the probability of repelling an intercepted attacker. The MOE's are, in effect, performance measures.

It is useful to group potential CM's into five interrelated categories: intrusion deterrents, component hardening, intrusion detection, alarm assessment, and reaction force. These CM categories, their MOE's, and explanations are given in table II. The MOE's follow readily, as a direct extension, from the interaction modeling.

TABLE II. MEASURES OF EFFECTIVENESS (MOE's) OF COUNTERMEASURES

CM category	MOE	Explanation
Intrusion deterrents	Δt_t	Barrier penetration delays increase attacker's time to reach target.
Component hardening	$\Delta t_{d/d}$	Making component less accessible/ more resistant to damage increases time to destroy it.
Intrusion detection	$-\Delta t_d$	Enhanced visual detection/electronic sensor modes decrease time till detection.
Alarm assessment	$-\Delta t_a$	Enhanced direct viewing/CCTV modes decrease time till assessment.
Reaction force	$-\Delta t_r$	Enhanced state of readiness for dispatching force decreases its response time.
	ΔP_r	Enhanced potency of force increases its probability of repelling an intercepted attacker.

It is desirable, for the reasons given in section 6, to transform the MOE's of intrusion detection and alarm assessment CM's to an increased probability of detection and valid alarm assessment. In other words, $-\Delta t_d$ and $-\Delta t_a$ are combined and transformed into ΔP_d, the increased probability of detection (and valid assessment). Again, it is assumed that when detection (and assessment) occurs, it occurs instantaneously upon perimeter penetration. For convenience, table III summarizes the revised MOE's of the CM categories.

TABLE III. REVISED MEASURES OF EFFECTIVENESS (MOE's) OF COUNTERMEASURES

CM Category	MOE
Intrusion deterrents	Δt_t
Component hardening	$\Delta t_{d/d}$
Intrusion detection (and assessment)	ΔP_d
Reaction force	$-\Delta t_r, \Delta P_r$

8. COST-BENEFITS OF COUNTERMEASURES

To evaluate the relative merits of comparable CM's, their cost-benefits may be compared. The benefit attributable to a CM may be described quantitatively by its MOE. The CM costs of concern are the total life-cycle costs. These costs include not only the procurement, installation, and maintenance costs, but consider the expected useful life and salvage value as well. However, the procurement and installation costs normally suffice when evaluating the cost-benefits of comparable CM's.

As previously explained (sect. 6), there is a crucial demand placed on the site's security system: the reaction force must intercept the attacker before he has completed his sabotage mission. To comply with this requirement, it may be necessary to augment the capabilities of the existing system with CM's. Once it has been determined that the intercept criterion can be satisfied with certain CM's, the system designer should seek the most cost-effective CM's and combinations thereof and still meet this criterion with an adequate margin of safety. The most cost-effective CM within a CM category is the one that causes the largest increment or decrement of time per unit cost to implement. (For intrusion detection, the cost-effective analogue is the largest increment of probability of detection per unit cost to implement.) Caution should be exercised when trying to compare the cost-benefits of CM's in different CM categories for the following reasons. Intrusion deterrent and reaction force CM's, which change the system's time parameters, are conceptually equivalent. But comparable equivalence does not extend to component hardening CM's, because such hardening applies only to a specific target. Even within the same CM category, the methodology may cause difficulties. Intrusion detection and alarm assessment were combined for convenience. In fact, the functions may be indistinguishable in the case of visual detection and (visual) assessment. However, there may be marked differences when detection is made by means of sensors, excluding closed-circuit television (CCTV).

Thus, the cost-benefit analysis methodology described for quantitatively evaluating potential CM's has certain potential pitfalls associated with it. Moreover, the mixed MOE's (Δt and ΔP_d) represent an additional impediment. For example, without a high P_d, the fact that the intercept criterion is satisfied may be inconsequential. On the other hand, a high P_d may be inconsequential if the intercept criterion is not satisfied. However, it is not currently practical to apply this methodology, because site data are lacking on the probability of intrusion detection and the reaction force's response time. To eliminate these data gaps would require an extensive test program entailing considerable time and cost. It therefore appears prudent to avoid this approach. An alternative reasonable approach is preferred; in such an approach, potential systems and CM's may be conceptualized through commonsense engineering judgments and insights.

9. RATIONALE

The rationale for defining a baseline security system consisting of the site's existing system augmented with appropriate CM's is embodied in several assumptions and approaches.

9.1 Assumptions

The following implicit assumptions are made in this study.

(a) There is no advance warning of an attack.* (Otherwise, the guard force could be strengthened, and troops might even be deployed around the site perimeter, making perimeter intrusion-detection sensors unnecessary.)

(b) The size of the site's guard force remains at its present level. (On one hand, manpower restrictions and personnel budgets prevent an increase in the number of military police or civilian guards. On the other hand, agreements with the host nations presumably prevent a reduction in the local-national guard force.)

9.2 Approaches

The following approaches will be taken.

(a) A coherent systems approach will be used to achieve a reasonable balance and effective integration of all elements in the physical protection system.

---

*Since effective counterintelligence can provide an advance warning of impending attack, it may be an excellent approach to curbing sabotage.

(b) Stress will be placed on CM's that are (1) relatively low cost, (2) universally applicable, and (3) easy to implement. (A stress on low cost seems prudent because of several factors: the budgetary constraints, the nature of the site's mission and the sabotage threat, the potential for alternative routings of messages, the technological and political changes that can alter the future nodal structure of the DCS, and the retrofit nature of the CM's. Note that easily implemented CM's are frequently low cost and in the nature of practices and procedures.)

(c) Methods and means of complementing and aiding the reaction force (guard force and backup force) will be sought so that this force can resist a sabotage attack more efficiently and effectively. (The objective is better use of limited manpower resources to combat sabotage.)

10. BASIC SYSTEM REQUIREMENTS

The basic requirements of the security system can be determined by carefully examining the interactions, which are sometimes subtle, among the system's elements. The following explanations may help some of these requirements to be understood.

(a) The attainment of the earliest possible intrusion detection, with high reliability, merits the highest priority, because detection is the first essential element in a sequence of defensive actions.

(b) Since the attackers will presumably seek targets outside the building areas, generally it will not be useful to implement intrusion-detection sensors beyond the immediate area of the perimeter barrier. This constraint on in-depth sensor deployment makes it mandatory that an extremely high P_d be realized within the confines of the perimeter barrier.

(c) If perimeter intrusion detection is to be made solely by visual means, the time it takes the attacker to penetrate a well-defined perimeter zone must be sufficient to assure a high P_d. This requirement dictates a double-fence barrier to delineate the perimeter zone.

(d) If perimeter intrusion detection is to be made by sensors, the time it takes the attacker to penetrate the inner boundary of a well-defined perimeter zone (following intrusion detection) must be sufficient to assure essentially instantaneous assessment with high probability. This requirement dictates a double-fence barrier to delineate the perimeter zone and to contain an integrated system of sensors.

11. POTENTIAL COUNTERMEASURES

CM's can increase a site's survivability to sabotage by reducing (1) the incidence of sabotage attacks and (2) the success rate of attempted attacks. (While it is also possible to minimize the consequences to the DCS of sabotage attacks that succeed, that subject is beyond the scope of this study.) The site's security system should thwart attempted sabotage through (1) early, reliable perimeter intrusion detection, and (2) prompt response by an able, armed reaction force to intercept and neutralize the attacker. CM's are designed to augment the site's capabilities and preparedness to curb sabotage. Basically, the CM's have three objectives: (1) earlier detection and assessment of perimeter intrusion, (2) earlier response and increased potency of the reaction force (on-site and remote backup force), and (3) increased time, manpower, and materiel needed by saboteurs to complete their mission.

Although it would be desirable to perform a quantitative cost-benefit analysis of potential CM's, as explained in section 8, it is not practical to do so at present because of critical data gaps. Therefore, a less restrictive, yet rational and meaningful, approach will be followed. It will be convenient to deal with potential CM's that are divided into four functional categories:

intrusion deterrents,
intrusion detection system,
component hardening, and
reaction force.

11.1 Intrusion Deterrents

A major category of potential CM's is perimeter intrusion deterrents. Some deterrents, whose effects are mainly psychological in nature, are chiefly effective against the nondedicated, poorly trained attacker (sect. 4). Others will even impede the dedicated, trained saboteur. A number of measures, if judiciously selected and integrated, go beyond the mere illusion of a strong perimeter defense posture. If an attacker who penetrates a perimeter barrier zone is sufficiently delayed in this zone, his risk of detection may increase substantially. Unfortunately, the most sophisticated type of double-fence barrier configuration can be penetrated in less than 2 minutes by a trained, skillful intruder who comes equipped with penetration aids.[1] The electrification of an inner fence may, however, significantly increase

[1] *Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)*

the attacker's time to penetrate the barrier. Still, it is doubtful that the "time window" available for intrusion detection would be sufficient to assure a high probability of detection by visual means--even assuming an elevated observation post with an unobscured view of the perimeter barrier zone, and a comparatively small perimeter. If the risk of nondetection is tolerable, however, this approach is preferred from a cost standpoint. Furthermore, it may also have some value in detecting a standoff attacker, who would not otherwise be detectable. But if the risk of nondetection is unacceptable, perimeter intrusion detection sensors must be installed in the perimeter barrier zone.

An effective barrier zone, which controls site access and inhibits unauthorized entry, consists of an integrated system of fences, gates, clear zones, intrusion warning, and lighting, as well as practices and procedures on vehicle parking and access control. The detailed recommendations that follow are largely derived from the Nuclear Weapon Security Manual.[4]

11.1.1 Types of Deterrents

Fences.--The perimeter barrier zone begins with a double chain-link fence that encloses the site, defines its boundaries, and impedes unauthorized entry into it. The fence barrier should delay an intruder sufficiently for the reaction force to respond in time. (When augmented with fence-mounted intrusion sensors, the fence should provide a positive means of detecting fence penetration.)

The site perimeter should be protected by a double chain-link security fence at least 2.1 m high and topped with at least three strands of barbed wire. The fences should be spaced about 10 m apart in a level, cleared area extending about 10 m beyond the fences. The bottom of the fence should reach within 5 cm of firm, level ground and be anchored to concrete curbs or sills so that intruders cannot lift the fabric and penetrate beneath the fence. Alternatively, a 2.7-m fence may be installed with the bottom 0.6 m encased in a concrete footing in the earth. Soil surfaces near the anchor should be compacted, to prevent surface water from eroding loose soil and deflecting the anchor. Drainage structures and water passages that penetrate the barrier and which have a cross-sectional area greater than 620 cm^2 should be protected by welded bar grills. As an alternative, drainage structures may be constructed of multiple pipes each having a diameter of 25 cm or less.

---

[4] *Nuclear Weapon Security Manual (U), DoD 5210.41-M (1 July 1975). (CONFIDENTIAL)*

Gates.--The perimeter fence should have the minimum number of gates needed for vehicle and personnel access. Gates should be structurally comparable to the fence and provide the same penetration resistance. Gate traffic should be under the control of the security guards. A guard may be posted at the gate to control access. If it is unattended, the gate should be kept locked. An intercom may be provided for authorized visitors to identify themselves. A cipher lock may be used by site personnel to enter the protected area. The gate should be observable from inside a nearby building or observation post, and may be operated electrically from that point. A buzzer should be activated when the gate is opened or unlocked.

Clear zones.--If not limited by site boundary restrictions, an extended clear zone of about 10 m should be maintained on each side of the perimeter fence, to inhibit cover and concealment of an intruder. The clear zones should be free of all obstacles, topographical features, and vegetation higher than 20 cm. (The cleared area outside the fence may also inhibit concealment of a standoff attacker whose target may be a critical antenna feedhorn.)

Intrusion warning.--A "no trespass" warning should be provided to warn intruders that the area is restricted and trespassers may encounter deadly force. Warnings should be communicated visually, at least, by signs. However, audible warnings may also be given by direct voice challenge or with sound-amplification equipment.

Warning signs should be installed periodically along the entire perimeter fence and at each entry point, in order to be readily seen by anyone approaching the perimeter. Warning signs should not aid intruder concealment or significantly obstruct the view of the perimeter. In areas where English is one of two, or more, commonly spoken languages, the warning signs should be posted in English and the local language(s). Signs should clearly state the dangers of trespassing in restricted areas. However, the specific words used should be consistent with host nation requirements. The signs should not reveal the nature and purpose of the site. The signs should be

(1) at least 0.3 m high by 0.6 m wide,
(2) painted with reflective material,
(3) legible at a distance of 15 m, and
(4) positioned periodically on the outer fence at no greater than 30-m intervals.

Lighting.--The entire perimeter barrier zone, including the cleared areas beyond the fences, should be effectively illuminated to assure a high probability of intrusion detection and assessment at night and under conditions of poor visibility. The perimeter lighting should deter unauthorized entry and facilitate intrusion detection. The

perimeter lighting should not silhouette or highlight security patrols, nor should it blind sentries. The lighting should be under the control of the security force.

The lighting should be positioned within the site, along the entire perimeter. It should be configured to provide adequate illumination for personnel identification at entry control points and in the areas immediately surrounding the site, according to the following criteria:

(1) Perimeter lighting should be designed to enable security guards to detect persons throughout the region bounded by the inner perimeter fence to 9 m outside the outer perimeter fence. When new lighting systems are installed the fixtures should be positioned no closer than 2.4 m inside the inner (or single) perimeter fence.

(2) The lighting system should produce full lumen output within 5 s after it is energized by either the prime power source or the emergency generator. This requirement assumes incandescent lamps. A lighting system that uses high-pressure sodium lamps is described in section 11.1.2.

(3) The clear zones, which include the area between the fences when two are used, should be lighted to an intensity that permits the security force to readily observe persons in those areas.

(4) Failure of one or more lights in the perimeter lighting circuit should not affect the operation of the remaining lights.

(5) To minimize the visibility of site personnel during a covert attack, patrol roads or paths should not be lighted unless necessary to reduce driving or personnel hazards.

Vehicle parking.--Private vehicles should be parked in a designated area outside the perimeter fence, within view of the gate guard. Vehicles should not be parked within 6 m of a secure area or near critical components. Military vehicles should be secured inside the perimeter fence, but should not impede the view of the perimeter.

Access control.--Access to limited or exclusion areas should be controlled through positive identification of all personnel by means of

(1) a controlled picture badge system,
(2) a formal entry control roster, and
(3) a visitor escort system and register.

Entry into limited or exclusion areas should be restricted to authorized personnel. The number of personnel authorized access should be limited to those who need to perform assigned tasks, as well as service, construction, and emergency personnel (fire, medical).

Local nationals assigned to the site should be authorized to enter upon presentation of a valid gate pass (i.e., one issued and stamped by the site's Security Officer). Local nationals having official business within the facility should be authorized to enter and be escorted by U.S. military personnel. Other U.S. forces personnel, maintenance personnel, contract personnel, and all others, including local nationals desiring access to the facility, should obtain approval from the DCS Detachment Commander, to be authorized to enter. The DCS Detachment headquarters element should notify the Site Chief of expected visitors and their authorization to enter the facility. Upon arrival at the site, individuals should be required to present identification before entering the facility. Personnel requesting access to the site who have not obtained approval from the Commander, DCS Detachment, should be denied access until the Site Chief or senior man on duty can confirm access authority with the Commander, DCS Detachment.

11.1.2 Costs

The main costs associated with the perimeter barrier zone, besides intrusion detection sensors and CCTV for assessment, are embodied in the fence, vehicle barrier, vehicle gate, and lighting. The descriptions and estimated costs of these items, which follow, have been abstracted mostly from a Mitre report.[5]

Fence.--The chain-link fence includes the wire-mesh fabric attached under tension (horizontally) to vertical line posts, and the horizontal rails between the posts for bracing. The vertical line posts are spaced at 3-m intervals; at the corners and ends of the fence, slightly heavier posts are used and diagonal bracing is added. The horizontal rails, which brace the vertical posts and support the fence fabric, are installed along the top of the fence (one-rail configuration). The bottom 0.6 m of the fence is encased in a concrete footing in the earth. Barbed wire is installed on brackets mounted on top of the fence posts.

The estimated procurement and installation costs are $65/m for a 2.7-m-high fence (single) of 9-gauge wire, with a 0.3-m barbed-wire topping, and with the bottom 0.6 m of fence encased in a concrete trench. Included in the cost are 6 corner posts.

---

[5] *J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

Vehicle barrier.--To prevent a vehicle from penetrating a protected zone, a vehicle barrier may be erected. A possible barrier consists of a 2.7-m section of rail extending upward, with a 1.5-m segment of the rail encased in concrete in the earth. Adjacent rails are spaced 76 cm apart.

The total estimated procurement and installation costs are $165 per rail, or $217 per linear meter. The cost breakdown per rail is as follows: $90 for the 2.7-m section of rail, $25 for digging a 2- by 1/3-m-deep trench, and $50 for the concrete fill and rail supports.

Vehicle gate.--The vehicle gate is configured as a single-slide (cantilever-type) gate (attached to the chain-link fence just described), 6.1 m wide by 2.1 m high. The gate is composed of wire mesh fabric attached to two vertical line posts, and is braced with horizontal rails between these posts. The horizontal rails may be installed on the gate in the same configurations as on the fence. The gate is topped with barbed wire in the same manner as the fence. For additional protection against vehicle intrusion, two 2.1-m vertical steel railway rails may be attached to the gate between the posts. These rails are similar to those used as vehicle barriers.

The estimated cost of the vehicle gate, including barrier rails, can be broken down as follows.

2.1- by 6.1-m chain-link gate, installed	$700
Barbed wire and brackets, installed	20
Two 2.1-m railway rails, installed	240
total cost	$960

Lighting.--The perimeter lighting requirements given earlier (sect. 11.1.1) presumed visual detection (and assessment) of intruders directly by security guards. However, it is possible to design outdoor lighting that enables alarm assessment by security guards--either directly, or through video equipment. Such lighting provides a conventional visual detection capability, plus an important growth potential--that is, CCTV could be installed later for alarm assessment purposes.

The lighting system now described is designed for efficient operation in conjunction with CCTV, but it may be used only for security guards/ patrols until CCTV is installed. In essence, the lighting consists of 150-W high-pressure sodium (HPS) lamps, (high-intensity discharge lamps), mounted atop 9.1-m lamp poles, spaced 40 m apart. This light source is satisfactory both for direct vision and for television surveillance/alarm assessment. A TV camera equipped with a silicon-diode-array vidicon tube is compatible with this light source.

In contrast to incandescent lamps, which start and achieve full output immediately, HPS lamps have a finite restrike time and require a finite time to achieve full output (measured in minutes).[6] Therefore, if primary power fails, the lighting system should be automatically switched to an uninterruptible power supply (UPS).

The total estimated costs to purchase and install this lighting system is $1307 per pole or $33/m. The system consists of the following components: a 9.1-m steel pole with a bracket arm to which is attached a luminere, a 150-W HPS lamp, and ballast; a junction box; a distribution cabinet; a main disconnect safety switch; and cabling.

11.2 Intrusion Detection System

The paramount requirement of the security system is that its intrusion detection system provide early, reliable intrusion detection of the attacker--before he has completed his sabotage mission, and in time for the reaction force to intercept and neutralize him. In the worst-case situation, there is no warning and detection first occurs when the saboteur's explosives are detonated.

The likelihood of early detection of covert perimeter intrusions at surveyed sites cannot be determined without extensive testing. However, the probability of detection is presumably low, because of the general lack of (1) effective perimeter barrier zones, (2) centrally located observation posts, and (3) perimeter intrusion sensors. To increase the likelihood of intrusion detection, an effective perimeter barrier zone should be implemented and fully exploited. An effective perimeter barrier zone may, by itself, deter intrusion and reduce the likelihood of an attack (sect. 11.1). Its most tangible benefit, however, is its potential for enhancing the detection of intrusions. A good vantage point for observing the perimeter barrier zone is essential, if security guards are to reliably detect intrusions. However, perimeter intrusion sensors may also be needed. CM's are generally needed to augment the detection capabilities of the sites' existing security systems and to assure earlier, more reliable intrusion detection. These CM's are major elements in the intrusion detection system concepts now described.

---

[6] *Intrusion Detection Systems Handbook, Volumes 1 & 2, Sandia Laboratories SAND 76-0554 (Revised October 1977).*

11.2.1 System Concepts

Three intrusion detection system concepts may be postulated. These system concepts vary from the simplest, in which total reliance is placed on an unaided security guard for detection (and assessment), to the most complex, in which detection (and assessment) aids play a major role.

Unaided guard.--In the simplest system, intrusions are visually detected (and assessed) directly by a security guard at a centrally located observation post that provides an unobstructed view of the perimeter.* The observation post should provide a relatively safe, protected position from small-arms fire; it may take the form of an erectable tower topped with a shelter. On the other hand, depending on the configuration of the site, the observation post may be adapted from an existing microwave tower or building roof. An observation post that is centrally located and protected, with good perimeter visibility is also ideally situated for the guard (1) to control site access through an electrically operated gate, (2) to activate a general alarm, and (3) to dispatch and control the reaction force. The observation post may also have a limited potential for detecting an off-site marksman bent on shooting out antenna feedhorns not masked by radomes. The effectiveness of the observation post for detecting a standoff attacker will depend largely on the configuration of the site and its environs.

A potentially useful adjunct to this configuration is the use of pet dogs as watchdogs. The dogs could roam freely without danger of activating intrusion sensors, and they might alert site personnel to attempted intrusions.

Detection aids.--Despite good visibility from an observation post, the intrusion detection performance of an unaided observer might not be acceptable. In that case, the guard's detection capabilities should be augmented with intrusion sensors deployed inside the perimeter barrier zone. The sensors may be so effectively used that they become the primary means of intrusion detection. In that case the observer's role will change, and he will primarily assess intrusion alarms activated by the barrier sensors. By using devices instead of a human observer to sense intrusions, such potential human failings as poor training, poor motivation, and poor alertness may be avoided. Furthermore, a protected vantage point for instantly and effectively assessing alarms provides other benefits. It obviates the need for a guard patrol to make on-the-spot assessments and CCTV for aided visual assessment.

**Existing site guard posts, near the main gates, usually do not provide unobstructed view of the perimeter. Therefore, reliable visual detection of perimeter intrusion is not possible from such posts. Furthermore, these posts are easily accessible and vulnerable to armed attack.*

Detection and visual assessment aids.--At certain sites, depending on the configuration, the perimeter view from the observation post may be partially obstructed. Intrusion sensors must then be provided to protect the obscured segments of the perimeter against undetected intrusions. Furthermore, whenever intrusions are detected in those segments, the observer may have to dispatch a guard patrol or use CCTV for assessment. For rapidity of assessment, CCTV is preferred. To enhance the efficiency and effectiveness of security operations, it may be desirable to fully automate and to rely completely on CCTV for assessment. This concept allows considerable flexibility in the placement of the TV monitors. For example, the TV monitors can be in the site's operations center. In that case the intrusion detection and assessment operations become more economical from a manpower resources standpoint, because the person who assesses intrusion alarms may also perform other functions. Moreover, the intrusion-detection and assessment operations may be centrally controlled and coordinated with other site operations.

11.2.2 Major System Elements

The intrusion-detection systems described consist of as many as three major system elements: master surveillance control facility (MSCF)/tower, intrusion sensor system, and CCTV alarm assessment system. The reader is referred to the Intrusion Detection Systems Handbook[6] prepared by Sandia Laboratories for comprehensive information on the selection, procurement, installation, test, and maintenance of all major elements except the MSCF/tower.

11.2.2.1 Master Surveillance Control Facility/Tower

The MSCF is the manned observation post (shelter) atop the centrally-located tower. Basically, the MSCF and tower provide a protected vantage point for observing the perimeter and detecting (and assessing) intrusions and standoff attackers. However, the manned post may also be used (1) to control site access through a gate, (2) to activate a general alarm, and (3) to dispatch and control the reaction force. In the upgraded system in which perimeter intrusion sensors are used to augment the observer's detection capabilities, the MSCF also houses sensor control/display equipment. In addition, if CCTV is used to augment the observer's visual assessment capabilities, the MSCF also houses CCTV control/display equipment.

Based on written communication* and subsequent verbal clarification, the estimated procurement costs of the MSCF shelter and tower are as follows:

---

[6] *Intrusion Detection Systems Handbook, Volumes 1 & 2, Sandia Laboratories SAND 76-0554 (Revised October 1977).*

**Headquarters Electronic Systems Division (AFSC), Hanscom Air Force Base, MA. Letter OCB, 17 February 1978 with attachment to HDL (Subject: Cost and description data on PAVE SAFE components).*

MSCF shelter	$19,300
Tower:	
6.1 m	$ 9,800
12.2 m	$13,500
15.2 m	$16,000

Under consideration is the hardening of the MSCF using opaque and transparent armor plating (on all sides and the bottom) to withstand a 7.62-mm NATO round. The specifications for hardening are not yet defined, and the cost is unknown.

11.2.2.2 Intrusion Sensor System

The intrusion sensor system consists of an integrated set of sensors deployed in the perimeter barrier zone that connect to the sensor control/display equipment used by the security guard at the observation/monitor point.

Sensors.--A wide range of perimeter intrusion sensors is available. Sensor performance may differ according to the types of intrusions detected, the conditions that cause unreliable detection, the methods of defeat, and the causes of false alarms. Applicable perimeter sensors fall into three categories: buried-line, fence-associated, and free-standing-line sensors. At present, there is no single sensor that will detect all types of intrusions (e.g., fence climbing, fence cutting, tunnelling, etc) and have an acceptably low false-alarm rate over the large range of man-made and natural environments encountered. Judicious combinations of sensors, tailored to a specific site's environment, are required to assure that all types of intrusions are detected with an acceptably low false-alarm rate, despite attacker penetration aids. To achieve the high P_d, the low false-alarm rate, and the resistance to intruder CM's demanded of a viable security system, it may be necessary to employ as many as three different types of sensors in the intrusion-detection system. The selection of the most cost-effective sensors for a specific site is difficult because it depends on numerous factors: the cost per unit distance protected; the resistance to intruder CM's (individually and in an integrated detection system); and the P_d and the false-alarm rate in a composite environment that includes weather, topography, vegetation, soil, wildlife, traffic, seismic noise sources, and electromagnetic interference. Brief descriptions and cost estimates are given for three typical perimeter sensors: microwave-line, buried-line, and fence sensors.[5,*]

---

[5] *J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

**Headquarters Electronic Systems Division (AFSC), Hanscom Air Force Base, MA, letter OCB, 17 February 1978, with attachment to HDL (Subject: Cost and description data on PAVE SAFE components).*

The microwave-line sensor consists of a microwave transmitter beaming a signal over a cleared, level area to a tuned receiver. Intruder-induced variations in the amplitude of the received microwave signal are detected. Two comparable commercial units have total estimated costs (procurement and installation) that average about $2300.[5] If the units are installed to protect a 100-m perimeter gap, the estimated costs are $23/m.

A buried-line sensor consists of (1) a buried transducer cable to detect seismic or magnetic disturbances caused by perimeter intrusions and (2) an electronic signal processor to enhance intrusion detection while suppressing spurious alarms. The total estimated cost (procurement and installation), based on averaging the costs of two commercial units, is $74/m if the units are installed to protect only a 30-m perimeter gap. The total estimated cost of the comparable DoD-approved buried-line sensor (MAID/MILES) is $69/m, assuming the same 30-m gap and allowing for installation.* An additional cost incurred in ensuring proper operation of a buried-line sensor is the cost of soil stabilization. Soil stabilization entails clearing an area of vegetation, sieving the soil base to remove rocks and debris, and grading the topsoil to level the area. The estimated cost of stabilizing a strip of soil 30 m wide and 1/2 m deep is $125/m.

The DoD-approved Fence Disturbance Sensor (FDS) is a fence-mounted sensor designed to detect attempted penetrations of the fence.[1] With reasonable care in the installation and in the sensitivity adjustment of the FDS, good intrusion detection performance can be obtained with an acceptably low false-alarm rate. The FDS is a normally open mercury switch that is mounted on a fence post. Typically, 15 FDS's are connected in parallel to alarm a 42-m sector of fence, assuming that the posts are spaced 3 m apart. The estimated cost of the FDS is $7, or $2/m.*

---

[1] *Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)*

[5] *J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

**Headquarters Electronic Systems Division (AFSC), Hanscom Air Force Base, MA, letter OCB, 17 February 1978, with attachment to HDL (Subject: Cost and description data on PAVE SAFE components).*

Sensor control/display equipment.--The sensor control/display equipment is used to control the sensors and to display the sensor alarms to security personnel. This equipment is mainly housed in the MSCF, where it facilitates prompt, reliable detection by the security guards of covert perimeter intrusions. To accomplish this function, sensor alarm data are collected, encoded, multiplexed, and securely transmitted via hardwire (buried cable) to the MSCF. There, the data are decoded and effectively displayed. Fail-safe and anti-tampering features are incorporated in the communications system. An emergency backup power supply enables the system to operate for a limited time if primary power fails. Since the equipment is modular in design, an individual user's requirements can be easily met. For example, a supervisory monitoring station may be easily configured.

The DoD-approved version of this equipment is called SPCDS (Small Permanent Communications and Display Segment). The SPCDS consists largely of a coder-multiplexer, sensor data (CMSD) and a receiver terminal (the communications and monitor-display equipment). A CMSD gathers data transmitted by buried cable from up to 79 sensors and from a line used for sensing tamper alarms and loss of fail-safe signals; it then encodes the data and transmits them via cables to one or two receiver terminals (in the MSCF and Central Security Control). A receiver terminal includes the hard-wire receiver, the digital-to-digital converters, the line supervision and alarm displays, and the power supply. It decodes the data and routes the message to either the line supervision display or the alarm display functional area. A geographic display facilitates alarm assessment. The estimated procurement costs of a CMSD and an SPCDS receiver terminal in the MSCF are as follows:*

CMSD. sensor data collector	$9,100
SPCDS 80-channel receiver terminal in the MSCF	$35,000

11.2.2.3 CCTV Alarm Assessment System

A CCTV alarm assessment system may be used by security personnel to accurately and rapidly assess intrusion alarms when segments of the perimeter are obscured or are not readily visible from the observation/monitoring post. Under certain adverse weather conditions, however, CCTV may be ineffective and direct visual assessment by a security patrol may be necessary. The CCTV alarm assessment system consists of CCTV cameras at the perimeter barrier zone that connect to the CCTV control/display equipment at the observation/monitoring post. CCTV cameras and lenses convert the optical scene to a video signal which is transmitted to the observation/monitoring post where it may be viewed in real time or recorded and played back later.

**Headquarters Electronic Systems Division (AFSC), Hanscom Air Force Base, MA, letter OCB, 17 February 1978, with attachment to HDL (Subject: Cost and description data on PAVE SAFE components).*

CCTV camera.--An appropriate CCTV camera/lens system can, with specified lighting (sect.11.1) yield a usable video signal of the region under observation. That signal can be transmitted to a remote monitor, where reliable alarm assessment can be made. As explained earlier, an HPS lamp and a camera equipped with a silicon-diode array vidicon tube are a cost-effective, compatible combination.

The video assessment system should provide sufficient resolution to recognize a human presence and to detect a small animal in the perimeter barrier zone. The Sandia Laboratories Handbook [6] gives design details and guidelines for selecting a camera/lens system that is compatible with the geometry of the perimeter barrier zone and target resolution requirements. A 1-in. format image tube and 1-in. format lens are desirable from a resolution standpoint. Since the focal length of the lens is determined by the maximum range at which the smallest object must be resolved, it is site dependent. It is desirable to design the camera/lens system to provide the barrier zone coverage needed and to meet the object resolution requirements with a minimum number of cameras. To implement a cost-effective system, it is necessary to judiciously design an integrated system considering the barrier zone geometry, intrusion sensor resolution, lighting, lens parameters, and camera placement.

A typical camera/lens system[5] is equipped with a fixed-focus lens (f 1.8, 75 mm) and a 1-in. silicon target vidicon, and it is enclosed in an environmental housing for protection against the weather and dust (a heater and blower are optional additions to extend the low-temperature operating range). The complete camera unit is installed on a 3-m high aluminum pole whose base is embedded in concrete. The costs of these components are estimated as follows.

Camera, lens, and environmental housing	$2703
3-m aluminum poles, installed	350
Installation (including junction boxes, connectors, and cabling)	4415
total cost	$7468

[5] *J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

[6] *Intrusion Detection Systems Handbook, Volumes 1 & 2, Sandia Laboratories SAND 76-0554 (Revised October 1977).*

CCTV control/display equipment.--The CCTV control/display equipment in the observation/monitoring post is linked to the CCTV cameras via a transmission system of video/control cabling and signal conditioning equipment. The control/display equipment basically consists of (1) video monitors, similar to home TV receivers, for assessing alarms and (2) auxiliary video switching equipment for interfacing the cameras and monitors. Since the alarm assessment system normally uses more cameras than display monitors, video switchers are needed to effectively interface multiple cameras with one or more monitors. A sequential switcher enables the video outputs from many cameras to be sequentially displayed at one monitor until an intrusion alarm occurs. At that point, the normal sequencing pattern is interrupted, and the camera which views the scene in the alarmed sector is automatically displayed on the monitor. Multiple alarms may be similarly processed. However, additional monitors or priority switching control may be required. A high density of alarms may overload the alarm assessment system and require direct visual assessment by a security patrol. The camera display/control console may be expanded to provide such optional equipment and features as video motion detection, video recording, and pan/tilt and zoom lens controls (if the CCTV cameras incorporate these features). However, such features are considered nonessential and would add considerably to the complexity and cost of the equipment. As in the intrusion sensor system, fail-safe and anti-tampering features should be provided as should emergency backup power.

The configuration and cost of the CCTV control/display equipment cannot be determined without first conducting a detailed systems engineering design involving (1) the perimeter barrier zone and (2) the intrusion detection system, including the alarm/assessment concept and implementation. Such considerations are necessarily site dependent. Nevertheless, it is possible to describe and estimate the costs of certain basic components. For example, a typical video monitor may feature a 12-in. picture tube, all solid-state circuitry, and brightness, contrast, and hold controls. A typical sequential switcher may handle as many as 20 or more cameras and enable the video output to be looped to a second monitoring location via a local switcher. The costs of these typical components are estimated as follows.[5]

Monitor	$319 ea.
Switcher (8 position)	$770 ea.

[5]*J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

The total cost will reflect the total number of these components needed plus their installation cost. Furthermore, the total cost must include the cost of the modular console, its installation, and testing.

11.3 Component Hardening

Component hardening has already been extensively studied,[1-3] and it will not be restudied here. Nevertheless, certain salient points merit discussion here. Component hardening means making the susceptible components of the communications system less accessible and more resistant to damage. In effect, component hardening increases $t_{d/d}$ (section 6), the time it takes the attacker to damage/destroy the component on reaching it. Component hardening may be necessary in case the reaction force is not otherwise timely or potent. The objective of hardening a component is to delay the saboteur sufficiently for a potent reaction force (section 11.4) to intercept him, before he can sabotage that component.

Certain components are also vulnerable to attack from outside the site. A component hardening program should give the highest priority to protecting those critical components that are directly vulnerable to attack from outside the site by small-arms fire, grenades, satchel/shaped charges, and explosives-laden vehicles. For example, normally visible antenna feedhorns should be obscured with opaque radomes. Buildings that house such critical components as AUTOVON and AUTODIN switches may be near the perimeter fence, where they are vulnerable to bombing. A good solution to this problem may be to erect protective revetments. When large aboveground fuel tanks are near the fence, acceptable CM's may take the form of revetments or tank burial. Of course, the possibility of expanding the site's boundary and reconfiguring the fencing should be considered. While these examples illustrate the interrelationship between the perimeter barrier zone and component hardening, the impact on perimeter visibility should also be considered.

---

[1] *Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)*

[2] *Murry B. Ginsberg et al, Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977). (FOUO)*

[3] *Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)*

Since microwave towers may be especially crucial to communications operations, their protection may merit special attention. Besides considering the installation of concrete sleeves around the legs of a self-supporting tower, the installation of a security fence and intrusion sensors (around the legs) also merits consideration.

Since a survivable communications node maintains its connectivity (via one or more links) to at least one other node, truly redundant (independent) links foster survivability. Redundancy implies an inability to simultaneously sever all links. Unfortunately, such severing is possible at *some* sites, where links are easily accessible through a single, unlocked manhole cover outside a secured building. It can be deduced that cable links should be rerouted to prevent simultaneous access at a single exterior point or, at least, that that access point should be well secured.

11.4 Reaction Force

The reaction force may be defined as the on-site security police and guards, and its local and remote backup force, who respond to unauthorized intrusions. The objective is to intercept and neutralize a saboteur before he can complete his mission or, at least, to delay him until needed reinforcements arrive. A timely and potent reaction force is evidently essential for curbing sabotage.

11.4.1 Timeliness

Whether or not the reaction force can achieve timely intercept of an attacker depends on four factors: (1) prompt, reliable intrusion detection, (2) significant delay of an attacker (attributable to barriers and component hardening measures), (3) reliable communications to promptly mobilize the reaction force, and (4) the reaction force's preparedness to promptly mobilize to confront an attacker.

11.4.2 Potency

Whether or not a reaction force that has achieved timely intercept of an attacker can also neutralize or delay him until reinforcements arrive depends on its strength. The force's strength depends mainly on three factors: (1) its size, (2) its preparedness (training, morale, and motivation), and (3) its armament and equipment.

Size.--Even a suitably equipped and trained reaction force must be at least half the size of the attacker force to successfully stall it until reinforcements arrive.[7]

---

[7] *W. Marcuse and J. P. Indusi, Simulating Physical Protection Against Overt Attacks at Facilities Using, Processing, or Storing Nuclear Materials, Journal of the Institute of Nuclear Materials Management (Fall 1975), 233-245.*

Preparedness.--If the reaction force is adequately staffed, armed, and equipped to neutralize or delay an attack force, its success will depend largely on the training, morale, and motivation of the group. The training should, in part, sensitize site personnel--especially security personnel--to the threat of sabotage. To effectively thwart an attacker, security personnel should first be fully indoctrinated in all aspects of the security system: the hardware, practices, and procedures. This training should initially instill a measure of confidence in the system's ability to detect and repel an armed attack. Training exercises entailing sabotage alerts and simulated sabotage attacks should be conducted periodically to enable site personnel to develop the necessary skills and proficiency in curbing a sabotage attack. Because such exercises build confidence, they should enhance the morale and motivation of site personnel and develop the reaction force into an effective counterforce. Furthermore, these exercises should demonstrate the effectiveness of the security system.

Armament and equipment.--The reaction force must, at least, be minimally armed and equipped to effectively thwart an armed attack. To withstand an armed assault by the attack force, the reaction force must be comparably well armed. Sidearms are required as a minimum. The security police and guards should be armed while on duty to facilitate an expeditious response, or they must have ready access to arms and ammunition so that their arming time is minimal. Since current practices and procedures at the sites generally inhibit the rapid arming of personnel, they should be revised.[3]

Guards who patrol the site perimeter or are posted near the perimeter fence may be vulnerable to a covert, surprise attack. Therefore, they need a duress alarm to surreptitiously and instantly alert security control of an immediate danger/attack.

The reaction force should be under effective command and control to be an effective counterforce to the attacker. Therefore, a hand-held portable radio for maintaining reliable two-way communications with security control, via a base radio station, should be provided (1) to each security patrol that conducts a routine patrol of the perimeter or directly assesses an intrusion alarm, and (2) to the reaction force attempting to intercept an intruder.

---

[3]*Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)*

To summarize, the alarm and communications equipment needed to augment the capabilities of the reaction force/security control consists of three items: (1) a duress alarm, (2) a hand-held portable radio, and (3) a base radio station. These items are commercially available; their estimated costs follow.[5]

(1) Duress alarm

A duress alarm is needed when security force personnel cannot overtly request aid because an armed intruder is present. A pocket-sized alarm, which is a completely self-contained radio transmitter (including its internal antenna), is available in two versions: a panic button (alarm coded) mode, and a sensor-operated voice mode. The estimated cost of the alarm-coded transmitter is $655.

(2) Hand-held portable radio

A hand-held portable radio is needed for the reaction force/security patrol to maintain reliable two-way communications with security control. The hand-held, vhf-FM transceiver is designed with integrated circuit plug-in modules for enhanced reliability and maintainability. The two-way radio operates from a rechargeable battery pack and can withstand severe weather conditions, including a wide range of ambient temperatures. It may also be adaptable to mobile operation. The estimated cost of the radio ($1159), which includes the cost of a battery charger, is based on averaging the costs of two commercially available units.

(3) Base radio station

A base radio station functions as the transmitting and receiving control center. It can communicate with on-site hand-held and vehicle-portable radios as well as with off-site radios (when seeking backup support). The vhf-FM base radio generally transmits about 100 W of rf power into an antenna located about 30 m above the local terrain. The estimated cost of the base radio station ($3389), which includes the cost of an omnidirectional antenna with transmission line, is based on averaging the costs of two commercially available units.

[5] *J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

11.5 Miscellaneous

Provision should be made for security control to activate loud emergency siren(s) for the general alerting and rapid mobilization of all site personnel, including security personnel, when there is a threat of immediate danger/attack. An "all-out" alert can be generated with a heavy-duty compressor type air trumpet installed on a 9-m-high aluminum pole. The double-projector trumpet connects directly to an air compressor which is driven by a motor. The estimated cost of this signaling system can be broken down as follows:[5]

Air trumpet	$ 675
Aluminum pole	$ 400
Installation	$ 300
Total	$1375

Manpower costs for security operations are a legitimate cost of the security system. Such costs will not be considered, however, because they are largely dependent on whether or not (1) personnel assigned to security monitoring/control operations also perform non-security duties, and (2) local nationals are employed as security guards. However, an automated security system that is efficient, effective, and reliable should prove economical from a manpower standpoint.

Good security practices and procedures are essential for an effective security system. This subject has been extensively studied, and guidelines and checklists have been proposed for practices and procedures to enhance site survivability against acts of sabotage.[3]

11.6 Cost Summary

The estimated costs of potential elements in a site security system are described in various subsections throughout sect. 11 but, for convenience, are summarized in table IV. The reader may refer to the pertinent sections for more detailed descriptions of the elements and explanations of the costs. However, for convenience, the following added information is listed here.

---

[3] *Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)*

[5] *J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).*

a. A double fence is needed to delineate the perimeter barrier zone.

b. The outdoor perimeter lighting is suitable both for direct visual detection and for CCTV alarm assessment. The lamp poles are spaced 40 m apart.

c. The MSCF (Manned Surveillance Control Facility) shelter atop the tower is an alternative to a fully automated intrusion-detection/assessment system that is monitored/controlled from a location in the site's operations center, for example.

d. Soil stablization is necessary for effective operation of the buried-line sensor.

e. For alarm assessment purposes, four or more CCTV cameras are needed for complete coverage of a site's perimeter.

f. The number of monitors and switchers required depends on the detailed characteristics of the site and its security system.

TABLE IV. ESTIMATED UNIT COSTS OF POTENTIAL ELEMENTS IN A SITE SECURITY SYSTEM

Potential Element	Estimated Unit Costs (1977 $)
Fence (single)	65/m
Vehicle barrier	217 per linear meter
Vehicle gate (with barrier)	960
Lighting	1,307 per pole, or 33/m
MSCF shelter (unhardened)	19,300[a]
Tower:	
12.2 m high	13,500[a]
15.2 m high	16,000[a]
FDS fence sensor	7, or 2/m[a]
Buried-line sensor:	
Commercial unit	$ 74/m (30-m gap protected)
MAID/MILES (DoD-approved)	$ 69/m (30-m gap protected)
Soil stabilization	125/m
Microwave-line sensor	23/m (100-m gap protected)
CMSD sensor data collector	9,100[a]
SPCDS 80-channel terminal in MSCF	35,000[a]
Closed-circuit television camera	7,468
Control/display equipment:	
Monitor	$ 319[a]
Switcher (8 position)	$ 770[a]
Duress alarm	655
Hand-held portable radio	1,159
Base radio station	3,389
Signaling system	1,375

[a] *Installation costs are not included.*

12. CONCLUSION

A cost-benefit analysis was made of potential CM's to enhance the survivability of DCS facilities to an attack by saboteurs. The interrelationships and the relative importance of the elements in a security system, whose level of sophistication was allowed to vary, were examined in detail. The costs of the various possible elements in the security system were estimated. It is necessary for the user to select a desired level of protection and requisite security system, duly considering the implementation costs.

LITERATURE CITED

(1) Harry A. Gieske et al, Impact of Sabotage on Defense Communications System Facilities: Phase I (U), Harry Diamond Laboratories TM-76-34 (December 1976). (SECRET)

(2) Murry B. Ginsberg et al, Impact of Sabotage on DCS Facilities: Phase II, Harry Diamond Laboratories TM-77-19 (October 1977). (FOUO)

(3) Murry B. Ginsberg et al, Impact of Sabotage on Manned DCS Facilities: Task I (U), Harry Diamond Laboratories TM-78-1 (November 1978). (SECRET)

(4) Nuclear Weapon Security Manual (U), DoD 5210.41-M (1 July 1975). (CONFIDENTIAL)

(5) J. M. Hockett et al, An Evaluation of Cost Estimates of Physical Security for Recycled Nuclear Fuel, Mitre Corp. MTR-3541 (January 1978).

(6) Intrusion Detection Systems Handbook, Volumes 1 & 2, Sandia Laboratories SAND 76-0554 (Revised October 1977).

(7) W. Marcuse and J. P. Indusi, Simulating Physical Protection Against Overt Attacks at *Facilities Using, Processing,* or Storing Nuclear Materials, Journal of the Institute of Nuclear Materials Management (Fall 1975), 233-245.

DISTRIBUTION

COMMANDER
US ARMY MATERIEL DEVELOPMENT
& READINESS COMMAND
5001 EISENHOWER AVENUE
ALEXANDRIA, VA 22333
ATTN DRXAM-TL, HQ TECH LIBRARY
ATTN DRCPA-S
ATTN DRCCE

ADMINISTRATOR
DEFENSE DOCUMENTATION CENTER
CAMERON STATION, BUILDING 5
ALEXANDRIA, VA 22314
ATTN DDC-TCA (12 COPIES)

COMMANDER
US ARMY RSCH & STD GP (EUR)
FPO NEW YORK 09510
ATTN LTC JAMES M. KENNEDY, JR.
CHIEF, PHYSICS & MATH BRANCH

COMMANDER
US ARMY MISSILE & MUNITIONS
CENTER & SCHOOL
REDSTONE ARSENAL, AL 35809
ATTN ATSK-CTD-F

DIRECTOR
US ARMY MATERIEL SYSTEMS
ANALYSIS ACTIVITY
ABERDEEN PROVING GROUND, MD 21005
ATTN DRXSY-MP
ATTN DRXSY-PO, COL A. A. DEPROSPERO

DIRECTOR
US ARMY BALLISTIC RESEARCH LABORATORY
ABERDEEN PROVING GROUND, MD 21005
ATTN DRDAR-TSB-S (STINFO)

PROJECT OFFICER
PHYSICAL SECURITY EQUIPMENT
7500 BACKLICK ROAD, BLDG 2089
SPRINGFIELD, VA 22150

DIRECTOR
DEFENSE CIVIL PREPAREDNESS AGENCY
WASHINGTON, DC 20301
ATTN F. VOGEL

DIRECTOR
DEFENSE COMMUNICATIONS AGENCY
DEPT OF DEFENSE
WASHINGTON, DC 20305
ATTN CODE 400
ATTN CODE 500
ATTN CODE 240
ATTN CODE 101B

HEADQUARTERS, DA
OCSA
WASHINGTON, DC 20310
ATTN DACS-DMO

DIRECTOR
COMMAND & CONTROL TECHNICAL CENTER
WASHINGTON, DC 20301
ATTN C670, F. MOORE

CHIEF, DEFENSE COMMUNICATIONS AGENCY
EUROPEAN AREA
APO NEW YORK 09131
ATTN ENGR DIV

CHIEF, DEFENSE COMMUNICATIONS AGENCY
PACIFIC AREA
WHEELER AFB, HI 96854
ATTN PLANS & PROGRAMS DIV

DIRECTOR
DEFENSE COMMUNICATIONS ENGINEERING CENTER
1860 WIEHL AVENUE
RESTON, VA 22090
ATTN CODE R200
ATTN CODE R300
ATTN CODE R700
ATTN CODE R720, JOHN WORTHINGTON

COMMANDER
US ARMY COMMUNICATIONS COMMAND
FT. HUACHUCA, AZ 85613
ATTN DCSOPS-PD
ATTN CC-OPS-OT, C. BREWINGTON

DEPARTMENT OF ENERGY
DIVISION OF SAFEGUARDS & SECURITY
WASHINGTON, DC 20545
ATTN S. R. GAARDER

COMMANDER
MERADCOM
FT BELVOIR, VA 22060
ATTN DRXFB-X, H. PETERS & J. BONETA

DEFENSE NUCLEAR AGENCY
NUCLEAR SECURITY DIVISION
WASHINGTON, DC 20305
ATTN LTC D. R. RICHARDS

US NUCLEAR REGULATORY COMMISSION
DIVISION OF SAFEGUARDS, FUEL CYCLE
& ENVIRONMENTAL RESEARCH
WASHINGTON, DC 20555
ATTN F. J. ARSENAULT

OFFICE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350
ATTN OP941-B

COMMANDER
NAVAL FACILITIES ENGINEERING COMMAND
ALEXANDRIA, VA 22332
ATTN JADREP OFFICE, 200 STOVALL ST

COMMANDER
1842d E. E. GROUP (AFCS)
RICHARDS GEBAUR AFB, MO 64030
ATTN EPELS

OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
WASHINGTON, DC 20305
ATTN NCS-PO (2 COPIES)

DEP CHIEF OF STAFF FOR
RESEARCH, DEVELOPMENT
& ACQUISITION (DCSRDA)
DEPT OF THE ARMY
WASHINGTON, DC 20310
ATTN DAMA-CSC, LT COL A. MADSEN

DEPUTY CHIEF OF STAFF FOR
OPERATIONS & PLANS (DCSOPS)
DEPT OF THE ARMY
WASHINGTON, DC 20310
ATTN DAMO-ODC
ATTN DAMO-ODM, LT COL A. MULARCIK

CHAIRMAN, PHYSICAL SECURITY
EQUIPMENT ACTION GROUP
UNDER SECRETARY OF DEFENSE FOR
RESEARCH & ENGINEERING
WASHINGTON, DC 20301
ATTN COL H. M. DIXON

DEP ASST SECRETARY OF DEFENSE
(SECURITY POLICY)
WASHINGTON, DC 20301
ATTN T. J. O'BRIEN

COMMANDER
US ARMY MOBILITY EQUIP R&D CTR
FT. BELVOIR, VA 22060
ATTN S. A. KILPATRICK

COMMANDANT
US ARMY ENGINEER SCHOOL
FT. BELVOIR, VA 22060
ATTN CAPT CANTRELL

COMMANDING GENERAL
US ARMY JOHN F. KENNEDY CENTER
FOR MILITARY ASSISTANCE
FT. BRAGG, NC 28307
ATTN GC-P-SP, MAJ C. GORDER

CHIEF OF ENGINEERS (DAEN)
DEPT OF THE ARMY
FORRESTAL BLDG
WASHINGTON, DC 20314
ATTN A. P. KNOCH

HEADQUARTERS USAF/SPP
BOLLING AIR FORCE BASE
WASHINGTON, DC 20336
ATTN MAJ J. E. SIEDLARZ

HEADQUARTERS AFCS
SCOTT AFB, IL 62225
ATTN LTC HIBSCHLE

COMMANDER
AIR FORCE SYSTEMS COMMAND (ESD/OCB)
HANSCOM AFB, MA 01731
ATTN R. E. O'NEIL
ATTN LTC W. K. MESSNER

COMMANDER
AFWL-SUL
KIRTLAND AFB, NM 87117
ATTN TECHNICAL LIBRARY

COMMANDER
ROME AIR DEVELOPMENT CENTER (AFSC)
GRIFFISS AFB, NY 13441
ATTN R. L. ALLEN

HEADQUARTERS US AIR FORCE
SECURITY SERVICE
SAN ANTONIO, TX 78243
ATTN SECURITY POLICE OPERATIONS DIV,
USAFSS/SPO

COMMANDER
HEADQUARTERS 7TH SIGNAL COMMAND
FT. RITCHIE, MD 21719
ATTN CCN-IS, W. A. KENT

HQ AEROSPACE DEFENSE COMMAND
DEPT OF THE AIR FORCE
ENT AFB CO 80912

COMMANDER
NAVAL TELECOMMUNICATIONS COMMAND
4401 MASS AVE NW
WASHINGTON, DC 20390
ATTN R. BERGER

DISTRIBUTION (Cont'd)

DEPUTY CHIEF OF STAFF FOR PERSONNEL
DEPT OF THE ARMY
WASHINGTON, DC 20310
ATTN DAPE-HRE, COL P. R. LOWREY
ATTN DAPE-HRE-CP, A. A. KLEKNER

COMMANDER
511TH MILITARY INTELLIGENCE
BATTALION (AEUMI/N/CE)
APO NEW YORK 09107
ATTN MR. DON FOSS

NAVSECGRU
3801 NEBRASKA AVE NW
WASHINGTON, DC 20390
ATTN G12

AIR FORCE SPACE AND MISSILE
SYSTEMS ORGANIZATION
WORLDWAY POSTAL CENTER
LOS ANGELES, CA 90045
ATTN YAS, MAJ DENNIS QUINE

THE AEROSPACE CORPORATION
P.O. BOX 92957
LOS ANGELES, CA 90009
ATTN DR. JULIAN REINHEIMER

COMMANDANT
US ARMY MILITARY POLICE SCHOOL
FT. MCCELLAN, AL 36205
ATTN ATZN-CDM-CE, LT LeVALLEY

THE MITRE CORPORATION
P.O. BOX 208
BEDFORD, MA 01730
ATTN J. M. HOCKETT

SANDIA LABORATORIES
P.O. BOX 5800
ALBUQUERQUE, NM 87115
ATTN J. D. WILLIAMS

WESTINGHOUSE ELECTRIC COMPANY
DETACHMENT 45
AF PLANT REPRESENTATIVE OFFICE
P.O. BOX 1693
BALTIMORE, MD 21203
ATTN FRANK BERTE

US ARMY ELECTRONICS RESEARCH
& DEVELOPMENT COMMAND
ATTN WISEMAN, ROBERT S., DR., DRDEL-CT
ATTN PAO
ATTN GINSBERG, M. B., DRDEL-AP-OA
(3 COPIES)

HARRY DIAMOND LABORATORIES
ATTN 00100, COMMANDER/TECHNICAL DIR/TSO
ATTN CHIEF, 00210
ATTN CHIEF, DIV 10000
ATTN CHIEF, DIV 20000
ATTN CHIEF, DIV 30000
ATTN CHIEF, DIV 40000
ATTN CHIEF, LAB 11000
ATTN CHIEF, LAB 13000
ATTN CHIEF, LAB 15000
ATTN CHIEF, LAB 22000
ATTN CHIEF, LAB 21000
ATTN CHIEF, LAB 34000
ATTN CHIEF, LAB 36000
ATTN CHIEF, LAB 47000
ATTN CHIEF, LAB 48000
ATTN RECORD COPY, 94100
ATTN HDL LIBRARY, 41000 (5 COPIES)
ATTN HDL LIBRARY, 41000 (WOODBRIDGE)
ATTN CHAIRMAN, EDITORIAL COMMITTEE
ATTN TECHNICAL REPORTS BRANCH, 41300
ATTN LEGAL OFFICE, 97000
ATTN LANHAM, C., 00210
ATTN WILLIS, B., 47400
ATTN OTTEN, M. G., 11140
ATTN MOORE, F. A., 15000
ATTN WALSH, G. W., 15000